A method ~~of controlling~~ the use of a smart card

Ins A1

The present invention concerns a method for controlling a smart card.

It applies more particularly to cards implementing cryptography algorithms using keys or pairs of keys in authentication sessions, during transactions between the card and a terminal.

Terminal means both the terminal in which the card is inserted, such as for example a payment terminal at a shop, and a bank server to which this payment terminal can be connected during a so-called direct connection transaction, according to a transaction mode known as "online" in British and American literature. This is notably the case with bank cards (debit/credit cards), for transactions relating to an amount which exceeds a certain threshold and in which the terminal is automatically connected to the server for additional checks before accepting the transaction.

Hereinafter, terminal means any external system to which the card is connected during a transaction.

The invention applies notably, but not exclusively, to smart cards of the electronic purse type, which are disposable or rechargeable payment means.

To prevent any fraud related to the use of smart cards, cryptographic algorithms are used, which use keys.

In practice, for a certain number of transactions, one or more authentication sessions by the card or terminal are provided for, so as to ensure maximum security. Authentication session means all the operations aimed at having the card or terminal calculate a signature (or certificate) corresponding to the application of a cryptography algorithm to a data item which may be imposed by one or other or a mixture of data of the card and terminal, and to the comparison of the two signatures. If this comparison is made by the card, it is an authentication by the card, which receives the signature calculated by the terminal. If it is an authentication by the terminal, the opposite is the case.

However, a new type of fraud has appeared which consists of deducing the value of the secret keys from statistical analyses based on measurements of current consumption in the card, during cryptographic calculation periods. This method of attack, known as DPA, standing for differential power analysis, is based on the fact that there are current consumption

signatures from which, if at least the data item applied as an input or the data item applied as an output is known, it is possible, by making assumptions on the keys, to find the value or part of the value of a key which was used in the cryptographic calculation in question.

To implement this fraud, it is therefore necessary to be able to initiate a cryptographic calculation with the same key a certain number of times, for example 300 times. For this to be useable, it is necessary to know or to be able to impose or to be able to fix a cryptographic calculation parameter.

If the example of smart cards of the electronic purse type implementing a secret key cryptographic algorithm is taken, the transactions between a card of this type and a terminal take place overall according to the following diagram, depicted in Figure 1:

- in an initialisation phase, the card calculates a session key SKX from a secret key KDX contained in the card concerned and a session counter NTX of the card which is incremented irreversibly during the transaction.

Then, according to the type of transaction, the card calculates a signature S1 and/or a signature S2, by applying the cryptographic algorithm to a data item, in general imposed by the card, and with the session key SKX.

For its part, the terminal calculates corresponding signatures, and, according to the type of transaction, either the terminal is authenticated by

the card, or the card is authenticated by the terminal. There is therefore a transmission of data and associated signatures during authentication sessions.

Take the case of an attempt at fraud based on a transaction of the loading type which normally serves for crediting the card of the electronic purse type with a certain sum.

If a transaction of this type is initiated a certain number of times (300 times for example) and the card is removed from the terminal just after the initialisation phase, the session counter NTX of the card will not be incremented. If 300 transactions of this type are made, removing the card from the terminal in order to abort the transaction, the session key SKX will be the same for these 300 transactions. It is therefore possible to collect 300 current consumption measurements curves corresponding to the calculation of 300 signatures on data which may be identical or variable according to the transaction, and with the same key.

Statistical analysis, where the data to which the cryptographic calculation is applied, are variable, makes it possible to obtain the session key.

According to the type of card, according to the transaction, it is possible in practice either to deduce the real secret keys contained in the card, or the session keys.

Knowledge of a real secret key makes it possible on the one hand to manufacture false cards with this key; these cards will be seen as good by a terminal.

This knowledge also makes it possible to perform transactions of the purchase cancellation type, for a card of the purse type, making it possible to recredit the card with a sum of money previously debited.

Knowledge of a session key for its part makes it possible to replay a transaction, using a false card (a clone) or a simulator.

The object of the invention is to prevent this type of fraud.

However, this fraud requires two distinct types of operation:

- an operation of collecting measurements of current consumption, for which it is necessary to use the card for making the measurements at propitious moments, with real transactions with a terminal, but which are aborted by pulling-out the card or transactions with a simulator of the terminal, transactions which will fail through lack of authentication of the terminal by their card (wrong signatures); and

- a statistical analysis operation using simulation means (computers), for finding the data sought, that is to say the keys.

To see through the statistical analysis, it is necessary to effect a large number of measurements: 50, 300, 5000.

This means that in the card there will be a large number of authentication session failures by the card, failures due to aborted transactions, by pulling-out the card from the terminal or which have fallen through

because of the supply by the terminal of wrong signatures.

Summary of the Invention

One object of the invention is thus to prevent the collection of current consumption measurements.

However, it has been seen that, in the case where it is sought to make this connection, there will be a large number of authentication session failures by the card.

One solution afforded to the technical problem of the invention consists of using in the card a control counter for counting down (or counting) these failures, and preventing the use of the card when a certain number of failures are counted.

~~The invention therefore concerns a control method according to Claim 1.~~

According to the invention, when a transaction between the card and a terminal which uses at least one authentication session by the card is initiated, the control counter is decremented by one unit. It is reincremented with this unit only if the authentication has succeeded. Or the control counter is incremented by one unit and is then decremented by this unit only if the authentication session has succeeded.

Preferably use is made of a control counter by key and/or by a pair of encrypting keys used in the card.

The control counter according to the invention can count down from or count up to a blocking value N representing the number of failures allowed.

This blocking value N depends on the type of transaction in which the associated key or pair of keys

is used. This value corresponds to a permitted number of times of transactions failed or aborted. In particular it takes account of the security level to be associated with the transaction, that is to say the risk incurred by a fraud on this key or pair of keys.

For example, where it is a question, with a card of the electronic purse type, of a transaction for updating parameters of the card, where these parameters can be the expiry date, the very values of the keys, a maximum sum for a transaction etc, a fairly low value N is provided for, since a very high degree of security must be associated with such a transaction and few errors in use can occur for this type of transaction. Where it is a case of purchase operations or cancellation of purchases, for which a certain number of incidents during the "normal" use of the card may occur, due notably to errors in use by the holder, a higher value is provided for.

For a given key or a given pair of keys, when the counter has reached its limit value, zero by decrementation or N by incrementation, the use of the key or of the pair of keys is blocked: no transaction using this key or pair of keys can any longer be effected. Preferably provision is made for this blocking to be irreversible. Provision can however be made for reinitialising the counter in the case where a blocking results indisputably from a non-intentional error by the user. Provision can also be made for being able to modify the blocking value N, if it proves in practice to be too low or too high. Such

reinitialisation or modification can be effected only according to a very secure procedure by an authorised third party (the bank).

In addition, in certain transactions, several cryptographic calculations are made, with the same key or the same pair of keys, up to and including the one consisting of the authentication session by the card. Provision is then made to decrement or increment the counter either by a new unit before each calculation or by a unit representing the number of calculations made. If the authentication session has succeeded, the counter is reincremented, or decremented, either by the sum of the units decremented, or incremented, by means of a pointing counter, or the representative unit, according to the chosen implementation mode of the control method according to the invention.

Brief Description of the Drawings

Other characteristics and advantages of the invention are described in the following description, given by way of indication and in no way limitatively, and with reference to the accompanying drawings, in which:

- Figure 1, already described, depicts a specimen diagram of cryptographic calculations made during a transaction between a card of the electronic purse type using a secret key cryptography algorithm and a terminal;

- Figure 2 is a general diagram of the resources of a card of this type, comprising control counters according to the invention; and

- Figures 3 to 5 are flow diagrams of typical transactions in an electronic purse application using the use control method according to the invention.

A Detailed Description

The general principle of the invention is to use at least one control counter which will be decremented or incremented by one unit at the start of a transaction between a terminal and a card, and which will be reincremented or decremented only after an authentication session by the card, if this session has succeeded.

Hereinafter only the case is taken where the counter is decremented systematically at the start of each transaction and reincremented subject to conditions. The converse case can easily be transposed to, where the counter is systematically incremented at the start of the transaction, and decremented subject to conditions.

The counter is initialised to a blocking value N, representing the number of permitted failures, which is notably a function of the application. If many transactions are started without allowing a successful authentication by the card, either because the transaction has been interrupted (the case of pull out), or because the data sent to the card to allow authentication by the card are false (the case of a simulator used in place of a true terminal), the counter which is decremented at each new transaction but which is not reincremented in all cases of failure in authentication by the card, finishes by reaching zero. Use of this card is then blocked.

An example of implementation of the invention will now be explained for a card of the electronic purse type using a cryptography algorithm whose encrypting key is a secret key. The invention is not limited either to this type of card or to this type of algorithm. It applies to any card effecting, for at least one transaction, an authentication session. The authentication session can use a secret key algorithm such as the DES algorithm, or an algorithm of the RSA type using a pair of encrypting keys (private key, public key). Some cards implement even these two algorithms in order to use one or other according to the transaction to be carried out. The control method according to the invention applies to all these different cards and applications.

Figure 2 depicts schematically the resources of a smart card of the electronic purse type, to which the control method of the invention can be applied.

It comprises principally a microprocessor μP, and memory resources including a read only memory ROM, containing in practice the program code, a dynamic memory RAM as a working memory and a non-volatile memory of the EEPROM type for example, which contains in practice sensitive parameters (in the security sense) of the card, including counters. In the example, this memory contains notably three secret keys denoted KDP, KDL and KDU, three associated session counters, denoted NTP, NTL and NTU, and three associated control counters according to the invention, denoted C_{KDP}, C_{KDL}, C_{KDU}.

This memory contains other parameters. Some can be updated by an external system, by means of an updating transaction, according to a secure procedure.

It should be stated that, in an electronic purse card, three types of transaction are possible and to each type of transaction there corresponds an associated secret key. There are thus the following types of transaction:

- Purchase or purchase cancellation with the associated secret key, denoted KDP;

- Load or unload with the associated secret key, denoted KDL, and

- Update with the associated secret key, denoted KDU.

In the invention, provision is then made for using a control counter by different secret key. There is thus the counter C_{KDP} associated with the secret key KDP, the counter C_{KDL} associated with the secret key KDL and the counter C_{KDU} associated with the secret key KDU.

The example of an operating flow diagram for such a card depicted in Figure 3 concerns a transaction of the purchase type, for which the card therefore uses the secret key KDP, the associated session counter NTP and the associated control counter according to the invention, C_{KDP}.

A purchase transaction comprises a first initialisation phase, which is normally limited by to the sending of a command by the terminal to the card, to specify the type of transaction to it. This command

is normally labelled as follows, in British and American literature: INIT FOR PURCHASE.

The microprocessor then switches to the address of the program code corresponding to this type of transaction.

In the invention, provision is made in this initialisation phase to decrement the control counter concerned, C_{KDP}, by one unit. The card therefore executes the following instruction: $C_{KDP} = C_{KDP} - u$.

It then tests whether the control counter has reached its limit value, zero in the example. If it has reached its limit value ($C_{KDP} \leq 0$), the card cannot carry on with the transaction, which will therefore terminate through lack of response from the card.

If the limit is not reached the card goes to a processing phase, in which it notably carries out the following operations:

- it calculates the session key SK_P, applying the cryptography algorithm to the value of the session counter NTP and using the secret key KDP,
- it sends a data item to the terminal so that it calculates a corresponding signature $S2_T$,
- it receives and returns the signature $S2_T$ calculated by the terminal,
- it calculates a signature S2, applying the cryptography algorithm to the variable data item sent to the terminal, with the session key SK_P.

The card then compares the two signatures. If they are comparable, the authentication has succeeded, and the control counter according to the invention is

then reincremented by the value u. Otherwise it is unchanged. The transaction can then continue.

It can be seen that, if too many transactions of the purchase type result in a failure in authentication by the card, the control counter according to the invention will make it possible to block any use of the card for a transaction of the purchase type.

In fact it blocks any use of the card for transactions of the same type, using the same secret key. Thus, in the case of the counter C_{KDP}, it is the purchase or purchase cancellation transactions which will be blocked.

Figure 4 shows an operating flow diagram for the card for the transaction of the purchase cancellation type, which therefore uses the same secret key KDP.

In this transaction, the initialisation phase initiated by an initialisation command for the terminal (command "init for purchase cancellation" according to British and American literature), comprises, in addition to the decrementation by one unit u of the control counter C_{KDP} according to the invention, the calculation of the session key SK_P and a signature S1 obtained by applying a cryptography algorithm to a data item, using the session key. At the end of this calculation, the card transmits this data item and the signature S1 to the terminal, to enable the terminal to authenticate the card. This authentication by the terminal is not the subject of any response from the terminal.

The card passes to the processing phase in which in its turn it authenticates the terminal, as before. In this type of transaction, the signature S2 is in general calculated on zero. The card therefore calculates the corresponding signature S2 with the session key KDP. It receives the signature $S2_T$ calculated by the terminal and makes a comparison of the two signatures. If they are comparable, the authentication session has succeeded. The control counter according to the invention is reincremented by the unit u. Otherwise the control counter is unchanged. The transaction continues.

In the case of this transaction, it can be seen that the card makes two cryptographic calculations up to and including that of the authentication session by the card, the calculation of the signature S1 and the calculation of the signature S2. For this transaction, provision is then preferably made for decrementing the control counter by a value corresponding to the number of cryptographic calculations made up to and including the one for the authentication session by the card.

This decrementation can take place on a single occasion, by a unit u representing this number of calculations performed for this transaction. The value taken by u for this transaction can be initialised in the initialisation phase, following the command of the "INIT FOR" type. This decrementation on several occasions, by decrementing the counter by one unit before each calculation, in the example, before the calculation of the signature S1 and before the

calculation of the signature S2. In this case, provision will be made for testing the limit value on the counter after each decrementation.

In this case also, there is also provided a pointing counter associated with the control counter, denoted D_{KDP} in Figure 2, initialised to zero at the start of the transaction, and which is for example incremented each time the control counter is decremented. Thus, if the authentication by the card has succeeded, the control counter is reincremented by the number contained in the pointing counter.

It should be noted that an expert will use one or other of the different possibilities of implementation according to the specificities of the application involved. Notably it is possible to use one implementation for one type of transaction and another for another type of transaction according to the degree of security required.

Figure 5 depicts an operating flow diagram for another type of transaction, the one of updating. It is relatively similar to the previous ones, but the authentication by the card takes place here on the signature denoted S1.

This is because, in general terms, the control counter is decremented at the start of the transaction. It is reincremented, if it can be, only after an authentication session by the card.

It should be noted that the flow diagrams in Figures 3 to 5 show only some of the operations performed during the transaction, for an explanation of

the method according to the invention. In practice, other operations are executed. Notably, according to the transactions, use is made, for calculating the signatures, of the current session key or the previous session key. After calculating the session key, the session counter must be incremented. All these aspects are specific to the application strictly speaking and have no interest with regard to the implementation of the control method according to the invention.

The different control counters must be initialised to a well chosen blocking value N. This value must take account of the associated type of transaction, the corresponding security level to be implemented but also possible errors during "normal" use by the card holder: it is not a question of blocking use of the card when the holder has not attempted to commit a fraud.

In one example for purely illustrative purposes, but which shows the different aspects which must taken into account, it is possible to initialise the control counter C_{KDP} associated with the purchase/purchase cancellation transactions at 100, the control counter C_{KDL} associated with the load/unload transactions at 20, and the control counter C_{KDu} associated with the update transactions at 10.

It was explained above that a variant of the control method according to the invention consists of incrementing the counter at each session and decrementing it only subject to conditions (authentication by the card successful). In this case, the counter is initialised to zero, and the limit

value, with which the content of the counter is compared, is equal to the blocking value N. Everything described above applies to this variant of the invention.

The invention has just been explained in an example of application to an electronic purse card. However, it is clear from this description that the control method according to the invention applies to any type of smart card provided that it performs an authentication session. This authentication session can be based on a secret key cryptography algorithm, for example of the DES type, as explained in the case of the electronic purse card, but also algorithms of other types, such as the algorithms of the RSA type using a pair of keys (private key, public key) for example. In addition, in the invention, smart card means both the cards to a well-known format and portable carriers.